

Malware

hoe kun je jezelf hier tegen beschermen?

De vraag

Naast phishing is malware één van de meest gebruikte vormen van 'cybercrime', ofwel digitale oplichting. Malware is simpelweg een verzamelnaam voor kwaadwillende software. Waar je bij phishing in een e-mail verleid wordt om vertrouwelijke informatie te delen, gaat malware een stap verder... het gaat namelijk zelf op zoek naar vertrouwelijke gegevens. Dit is mogelijk doordat er eerst op slinkse wijze kwaadwillende software op je pc wordt geïnstalleerd, zoals een virus. Deze software is bewust opgezet om computersystemen te verstoren of om bij gevoelige informatie op jouw pc te komen. Zo'n infectie kan dus zeer schadelijk en riskant zijn. Voor het bedrijf waar je werkt, maar ook voor jou als persoon. Zo kan men bijvoorbeeld door je toetsaanslagen te registreren en analyseren achter je bank- en inloggegevens komen. Maar ook is het mogelijk om je firewall of antivirusprogramma op afstand uit te schakelen, waardoor er nog meer kwaadwillende software op je computer kan worden geïnstalleerd. Hoe kun je jezelf hier nu tegen beschermen? En belangrijker, wat kun je zelf doen om te voorkomen dat deze kwaadwillende software op je computer wordt geïnstalleerd?

De uitdaging

Wat veel mensen niet weten is dat je de software vaak zelf installeert, zonder dat je dit in de gaten hebt. Dit kan bijvoorbeeld gebeuren doordat je bepaalde (onveilige) websites bezoekt of gratis software van internet download. En wist je dat een USB-stick ook een virus kan bevatten? Zo is een 'achtergelaten' USB-stick vaak een makkelijke bron van malware waar veel mensen intrappen. Om te achterhalen wie de eigenaar van de USB-stick is, stop je vaak goedbedoeld de stick in je laptop of pc. Dan is het kwaad al geschied en met een beetje pech is de schade onomkeerbaar. Net als bij phishing kan malware, ook per e-mail binnenkomen. Je wordt dan verleid om op een link te klikken of om vervuilde documenten te openen.

De oplossing

Voorkomen is natuurlijk beter dan genezen. De volgende tips kunnen je op weg helpen om je te beschermen tegen malware:

- ▲ Zorg voor een goed antivirusprogramma of goede anti-spam software op je laptop of PC. De grootste oorzaak van malware is vaak een 'gat' in je software. Maak het cybercriminelen dus zo lastig mogelijk door jouw systeem goed te beveiligen.
- ▲ Voer regelmatig een antivirusscan uit. Zorg daarbij dat je de meest recente versie van de scanner gebruikt. Zo blijft je systeem up to date en check je actief de veiligheid!

- ▲ Pas op met welke websites je bezoekt. Wanneer je onveilige websites bezoekt (zonder 'slotje' in de URL-balk) of sites waar je 'gratis' zaken kunt downloaden, zoals muziek of films, zet je de deur voor malware vaak wagenwijd open.
- ▲ Wees alert bij het openen van bestanden of links die je via e-mail ontvangt. Herken je de afzender niet, of komt de tekst in de e-mail niet vertrouwd over, dan kan het wel eens zijn dat de bijgevoegde link of het (zip-)bestand besmet is. De e-mail kan via een bekende relatie van je komen, dat maakt de techniek zo geraffineerd. Hier kun je simpel op reageren door de afzender te vragen of de mail bewust verstuurd en dus vertrouwd is. Zo niet? Verwijder dan direct de mail en doe voor de zekerheid een scan!
- ▲ Let op met het gebruik van USB-sticks. Zij kunnen de bron zijn van een besmetting. Gebruik daarom geen USB-sticks van een ander en kies zelf voor een speciale beveiligde (encrypted) USB-stick.
- ▲ Signaleer je verdachte (online) zaken op je werkplek? Meld dit dan direct bij je Chief Information Security Officer (CISO) of ICT-afdeling.

Tot slot... naast het voorkomen van malware is het ook goed om te herkennen wanneer je met malware te maken hebt. Malware kan namelijk 'op de achtergrond' aan het infecteren zijn, zonder dat jij er weet van hebt. Hoe sneller je de infectie aanpakt, hoe beter. Krijg je veel pop-ups tijdens het surfen op internet of is je pc aanzienlijk trager dan normaal? Is je startpagina gewijzigd of lijkt je computer een eigen leven te leiden door pagina's te openen waar jij niet om hebt gevraagd? Dan kan het weleens zijn dat je met een malware infectie te maken hebt. Kortom, herken je één van bovenstaande punten? Laat je apparaat dan uitgebreid controleren voordat het te laat is. Een gewaarschuwd mens telt immers voor twee.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak. Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.

